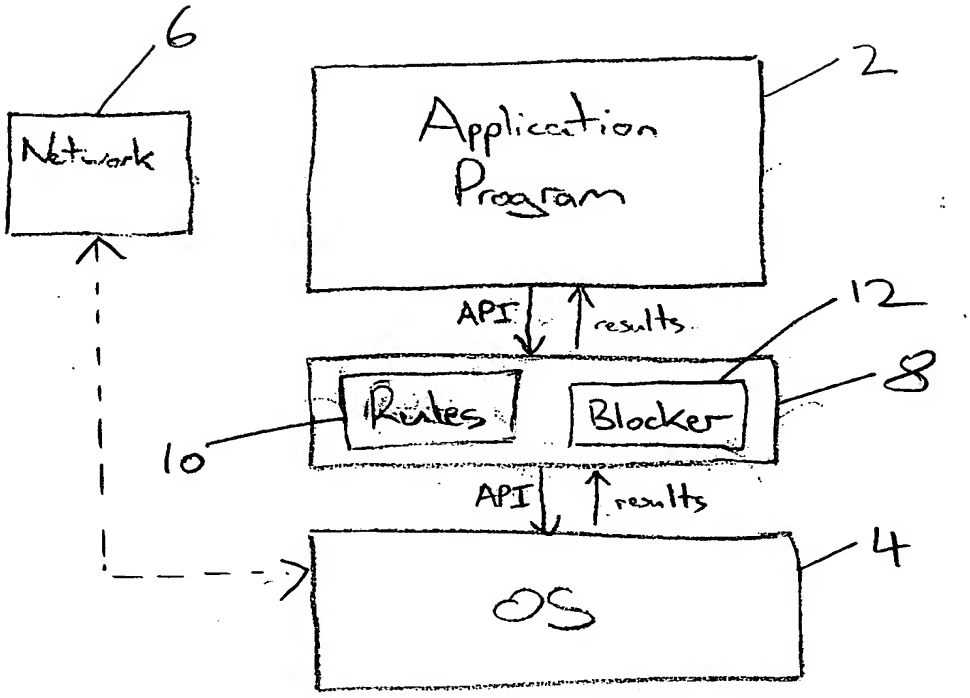
6
Network
Application Program
2
API
results
12
Routes
Blocker
8
10
API
results
OS
4

Fig. 1

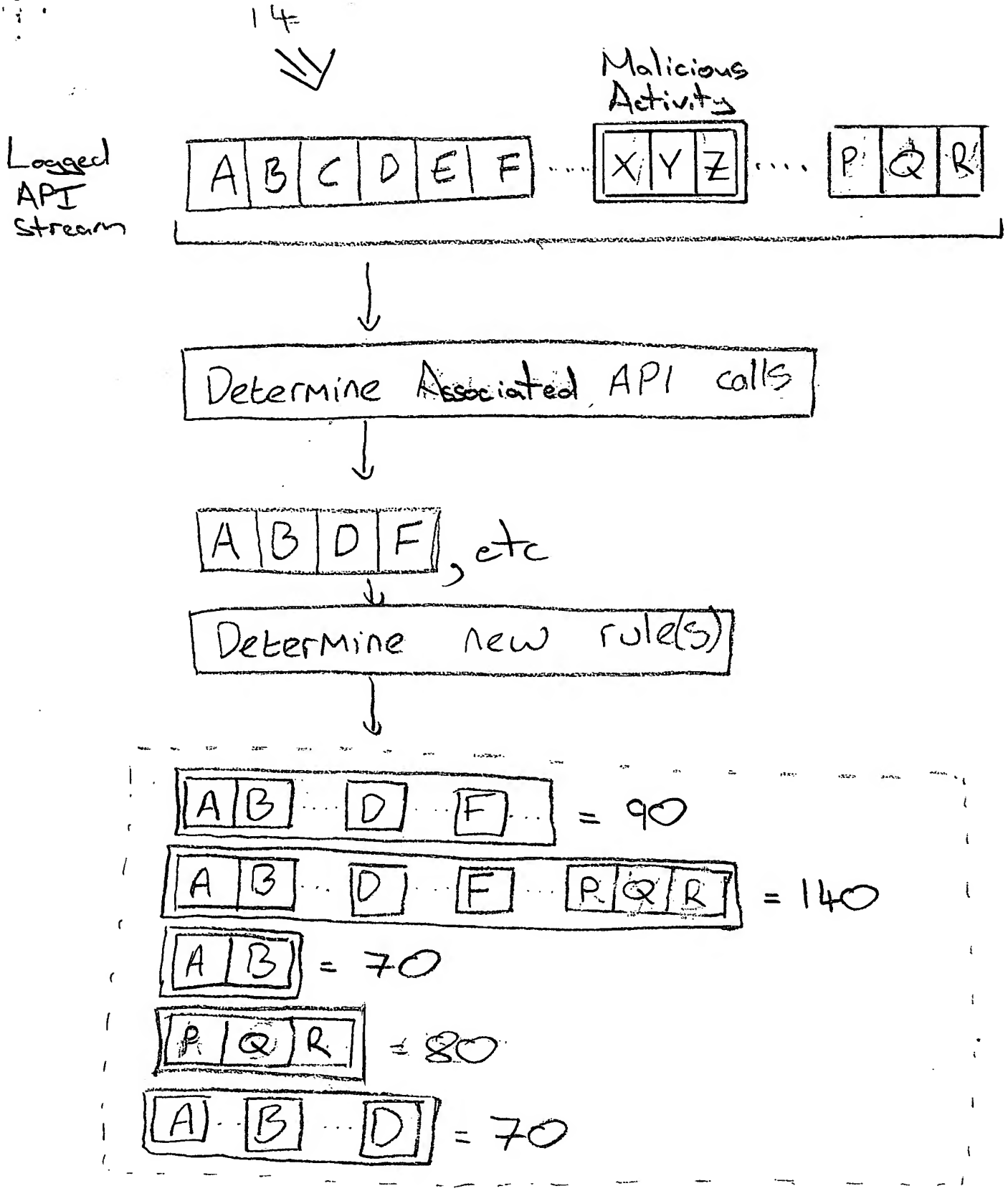
14
Malicious Activity
Logged API Stream
A B C D E F
X Y Z
P Q R
Determine Associated API calls
A B D F, etc
Determine new rule(s)
A B D F = 90
A B D F P Q R = 140
A B = 70
P Q R = 80
A B D = 70

Fig. 2

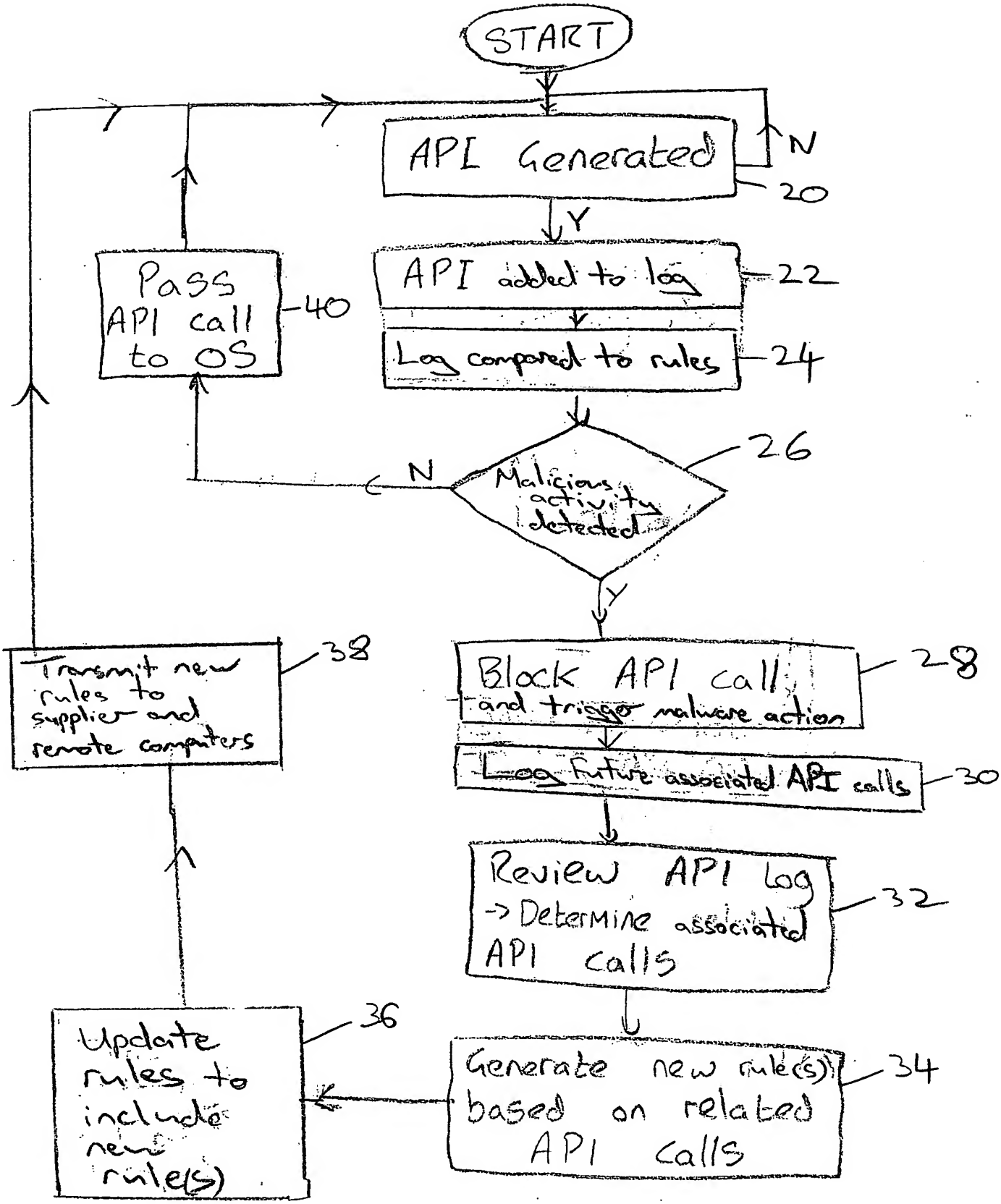
START
API Generated
N
20
Y
API added to log
22
Log compared to rules
24
Malicious activity detected
26
N
Pass API call to OS
40
Y
Block API call and trigger malware action
28
Log future associated API calls
30
Review API log -> Determine associated API calls
32
Generate new rule(s) based on related API calls
34
Update rules to include new rule(s)
36
Transmit new rules to supplier and remote computers
38

Fig. 3

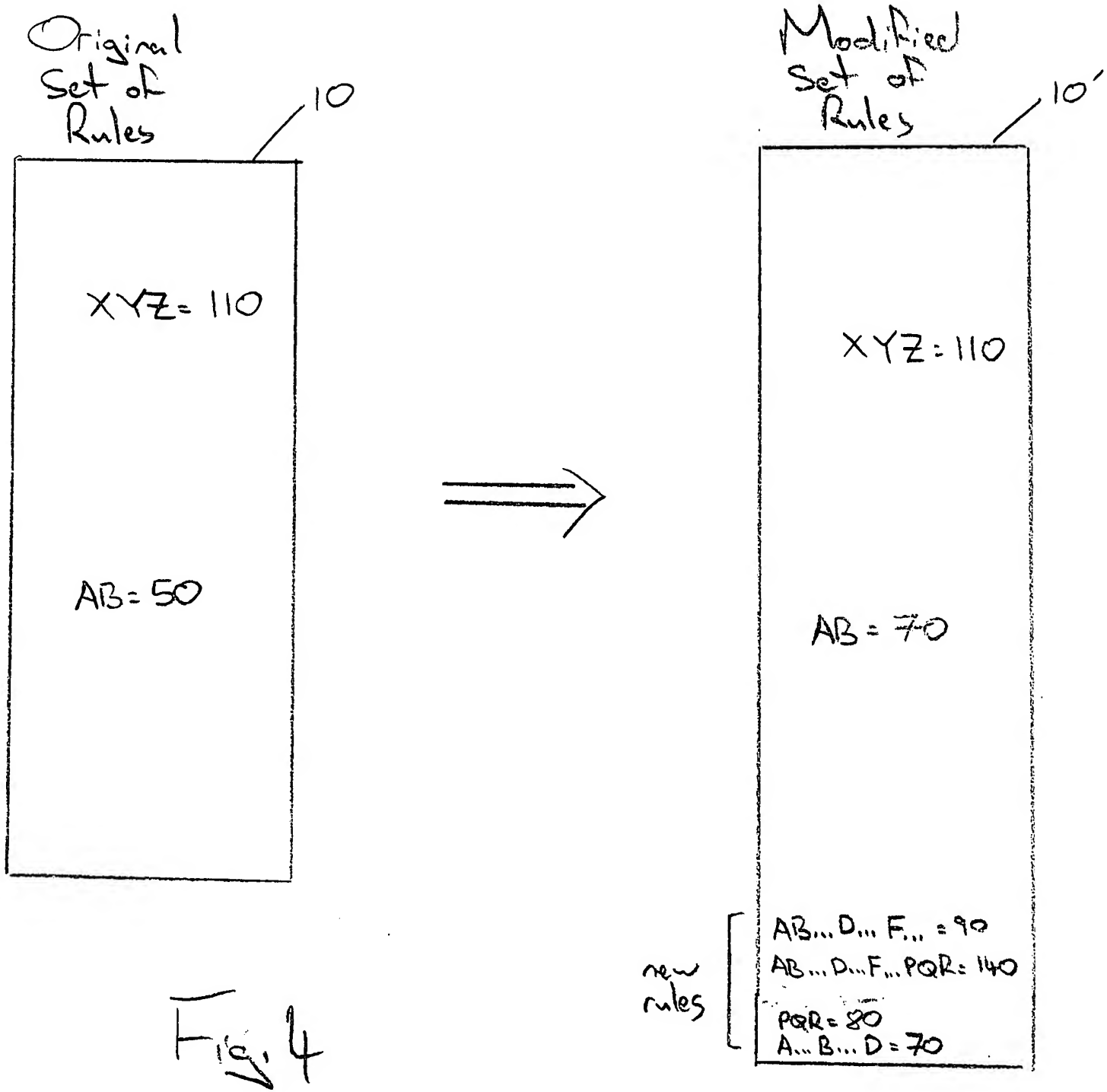
Original Set of Rules
10
XYZ = 110
AB = 50
Modified Set of Rules
10'
XYZ = 110
AB = 70
new rules
AB... D... F... = 90
AB... D... F... PQR = 140
PQR = 80
A... B... D = 70

Fig. 4

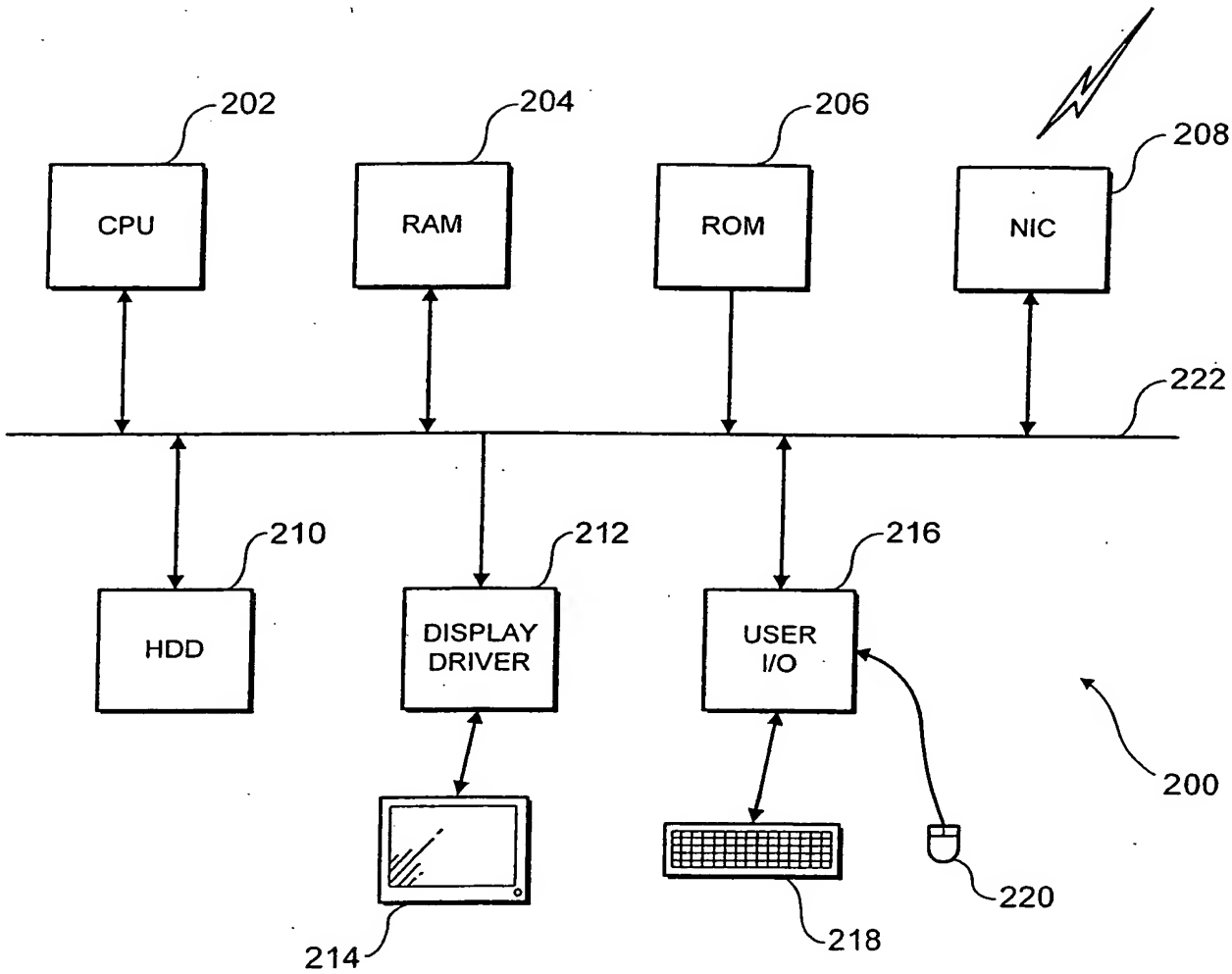
202
204
206
208
CPU
RAM
ROM
NIC
222
210
212
216
HDD
DISPLAY DRIVER
USER I/O
200
214
218
220

FIG. 5